De Finetti reductions

and parallel repetition of multi-player non-local games

joint work with Andreas Winter

Cécilia Lancien

Toulouse - StoQ - September 11th 2015

Outline

1. De Finetti type theorems
2. Multi-player non-local games
3. Using de Finetti reductions to study the parallel repetition of multi-player non-local games
4. Summary and open questions

Outline

1. De Finetti type theorems
2. Multi-player non-local games
3. Using de Finetti reductions to study the parallel repetition of multi-player non-local games
4. Summary and open questions

Classical and quantum finite de Finetti theorems

Motivation : Reduce the study of permutation-invariant scenarios to that of i.i.d. ones.

Classical and quantum finite de Finetti theorems

Motivation : Reduce the study of permutation-invariant scenarios to that of i.i.d. ones.

Classical finite de Finetti Theorem (Diaconis/Freedman)

Let $P^{(n)}$ be an exchangeable p.d. in n r.v.'s, i.e. for any $\pi \in \mathcal{S}_n$, $P^{(n)} \circ \pi = P^{(n)}$.
For any $k \leqslant n$, denote by $P^{(k)}$ the marginal p.d. of $P^{(n)}$ in k r.v.'s.
Then, there exists a p.d. μ on the set of p.d.'s in 1 r.v. s.t. $\left\| P^{(k)} - \int_Q Q^{\otimes k} d\mu(Q) \right\|_1 \leqslant \frac{k^2}{n}$.

$\rightarrow$ The marginal p.d. (in a few variables) of an exchangeable p.d. is well-approximated by a convex combination of product p.d.'s.

Classical and quantum finite de Finetti theorems

Motivation : Reduce the study of permutation-invariant scenarios to that of i.i.d. ones.

Classical finite de Finetti Theorem (Diaconis/Freedman)

Let $P^{(n)}$ be an exchangeable p.d. in n r.v.'s, i.e. for any $\pi \in \mathcal{S}_n$, $P^{(n)} \circ \pi = P^{(n)}$.
For any $k \leqslant n$, denote by $P^{(k)}$ the marginal p.d. of $P^{(n)}$ in k r.v.'s.
Then, there exists a p.d. μ on the set of p.d.'s in 1 r.v. s.t. $\left\| P^{(k)} - \int_Q Q^{\otimes k} d\mu(Q) \right\|_1 \leqslant \frac{k^2}{n}$.

$\rightarrow$ The marginal p.d. (in a few variables) of an exchangeable p.d. is well-approximated by a convex combination of product p.d.'s.

Quantum finite de Finetti Theorem (Christandl/König/Mitchison/Renner)

Let $\rho^{(n)}$ be a permutation-symmetric state on $(\mathbf{C}^d)^{\otimes n}$, i.e. for any $\pi \in \mathcal{S}_n$, $U_\pi \rho^{(n)} U_\pi^\dagger = \rho^{(n)}$.
For any $k \leqslant n$, denote by $\rho^{(k)} = \mathrm{Tr}_{(\mathbf{C}^d)^{\otimes n-k}} \rho^{(n)}$ the reduced state of $\rho^{(n)}$ on $(\mathbf{C}^d)^{\otimes k}$.
Then, there exists a p.d. μ on the set of states on $\mathbf{C}^d$ s.t. $\left\| \rho^{(k)} - \int_\sigma \sigma^{\otimes k} d\mu(\sigma) \right\|_1 \leqslant \frac{2kd^2}{n}$.

$\rightarrow$ The reduced state (on a few subsystems) of a permutation-symmetric state is well-approximated by a convex combination of product states.

De Finetti reductions (aka "Post-selection techniques")

Motivation : In several applications, one only needs to upper-bound a permutation-invariant object by product ones...

De Finetti reductions (aka "Post-selection techniques")

Motivation : In several applications, one only needs to upper-bound a permutation-invariant object by product ones...

"Universal" de Finetti reduction for quantum states (Christandl/König/Renner)

Let $\rho^{(n)}$ be a permutation-symmetric state on $(\mathbf{C}^d)^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{d^2-1} \int_\sigma \sigma^{\otimes n} d\mu(\sigma),$$

where μ denotes the uniform p.d. over the set of mixed states on $\mathbf{C}^d$.

Canonical application : If f is an order-preserving linear form s.t. $f \leqslant \varepsilon$ on 1-particle states, then $f^{\otimes n} \leqslant \mathrm{poly}(n)\varepsilon^n$ on permutation-symmetric n-particle states (e.g. security of QKD protocols).

De Finetti reductions (aka "Post-selection techniques")

Motivation : In several applications, one only needs to upper-bound a permutation-invariant object by product ones...

"Universal" de Finetti reduction for quantum states (Christandl/König/Renner)

Let $\rho^{(n)}$ be a permutation-symmetric state on $(\mathbf{C}^d)^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{d^2-1} \int_\sigma \sigma^{\otimes n} d\mu(\sigma),$$

where μ denotes the uniform p.d. over the set of mixed states on $\mathbf{C}^d$.

Canonical application : If f is an order-preserving linear form s.t. $f \leqslant \varepsilon$ on 1-particle states, then $f^{\otimes n} \leqslant \mathrm{poly}(n)\varepsilon^n$ on permutation-symmetric n-particle states (e.g. security of QKD protocols).

"Flexible" de Finetti reduction for quantum states

Let $\rho^{(n)}$ be a permutation-symmetric state on $(\mathbf{C}^d)^{\otimes n}$. Then,

$$\rho^{(n)} \leqslant (n+1)^{3d^2-1} \int_\sigma F\left(\rho^{(n)}, \sigma^{\otimes n}\right)^2 \sigma^{\otimes n} d\mu(\sigma),$$

where μ denotes the uniform p.d. over the set of mixed states on $\mathbf{C}^d$, and F stands for the fidelity.
$\rightarrow$ Follows from pinching trick.

What is the “flexible” de Finetti reduction good for ?

$$\rho^{(n)} \leqslant \mathrm{poly}(n) \int_\sigma F\left(\rho^{(n)}, \sigma^{\otimes n}\right)^2 \sigma^{\otimes n} d\mu(\sigma)$$

State-dependent upper-bound : Amongst states of the form $\sigma^{\otimes n}$, only those which have a high fidelity with the state of interest $\rho^{(n)}$ are given an important weight.
$\rightarrow$ Useful when one knows that $\rho^{(n)}$ satisfies some additional property : only states $\sigma^{\otimes n}$ approximately satisfying this same property should have a non-negligible fidelity weight...

What is the “flexible” de Finetti reduction good for ?

$$\rho^{(n)} \leqslant \mathrm{poly}(n) \int_\sigma F\left(\rho^{(n)}, \sigma^{\otimes n}\right)^2 \sigma^{\otimes n} d\mu(\sigma)$$

State-dependent upper-bound : Amongst states of the form $\sigma^{\otimes n}$, only those which have a high fidelity with the state of interest $\rho^{(n)}$ are given an important weight.
$\rightarrow$ Useful when one knows that $\rho^{(n)}$ satisfies some additional property : only states $\sigma^{\otimes n}$ approximately satisfying this same property should have a non-negligible fidelity weight...

Some canonical examples of applications :

- If $\mathcal{N}^{\otimes n}(\rho^{(n)}) = \tau_0^{\otimes n}$, for some CPTP map $\mathcal{N}$ and state τ_0, then

$$\rho^{(n)} \leqslant \mathrm{poly}(n) \int_\sigma F\left(\tau_0, \mathcal{N}(\sigma)\right)^{2n} \sigma^{\otimes n} d\mu(\sigma).$$

$\rightarrow$ Exponentially small weight on states $\sigma^{\otimes n}$ s.t. $\mathcal{N}(\sigma) \neq \tau_0$.

- If $\mathcal{N}^{\otimes n}(\rho^{(n)}) = \rho^{(n)}$, for some CPTP map $\mathcal{N}$, then there exists a p.d. $\widetilde{\mu}$ over the range of $\mathcal{N}$ s.t.

$$\rho^{(n)} \leqslant \mathrm{poly}(n) \int_\sigma F\left(\rho^{(n)}, \sigma^{\otimes n}\right)^2 \sigma^{\otimes n} d\widetilde{\mu}(\sigma).$$

$\rightarrow$ No weight on states $\sigma^{\otimes n}$ s.t. $\sigma \notin \mathrm{Range}(\mathcal{N})$.

In particular : if $\mathcal{X}$ is finite and $P^{(n)}$ is a permutation-invariant p.d. on $\mathcal{X}^n$, then there exists a p.d. $\widetilde{\mu}$ over the set of p.d.'s on $\mathcal{X}$ s.t. $P^{(n)} \leqslant \mathrm{poly}(n) \int_Q F\left(P^{(n)}, Q^{\otimes n}\right)^2 Q^{\otimes n} d\widetilde{\mu}(Q)$.

Outline

ℓ-player non-local games

ℓ cooperating but separated players. Each player i receives an input $x_i \in \mathcal{X}_i$ and produces an output $a_i \in \mathcal{A}_i$. They win if some predicate $V(a_1, \ldots, a_\ell, x_1, \ldots, x_\ell)$ is satisfied. To achieve this, they can agree on a joint strategy before the game starts, but then cannot communicate anymore.

ℓ-player non-local games

ℓ cooperating but separated players. Each player i receives an input $x_i \in \mathcal{X}_i$ and produces an output $a_i \in \mathcal{A}_i$. They win if some predicate $V(a_1,\ldots,a_\ell,x_1,\ldots,x_\ell)$ is satisfied. To achieve this, they can agree on a joint strategy before the game starts, but then cannot communicate anymore.

Description of an ℓ-player non-local game G

- Input alphabet : $\underline{\mathcal{X}} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_\ell$. Output alphabet : $\underline{\mathcal{A}} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$.
- Game distribution $=$ P.d. on the queries : $\{T(\underline{x}) \in [0,1],\ \underline{x} \in \underline{\mathcal{X}}\}$.
- Game predicate $=$ Predicate on the answers and queries : $\{V(\underline{a},\underline{x}) \in \{0,1\},\ (\underline{a},\underline{x}) \in \underline{\mathcal{A}} \times \underline{\mathcal{X}}\}$.
- Players' strategy $=$ Conditional p.d. on the answers given the queries : $\{P(\underline{a}|\underline{x}) \in [0,1],\ (\underline{a},\underline{x}) \in \underline{\mathcal{A}} \times \underline{\mathcal{X}}\}$.

$\rightarrow$ Belongs to a set of "allowed strategies", depending on the kind of correlation resources that the players have (e.g. shared randomness, quantum entanglement, no-signalling boxes etc.)

ℓ-player non-local games

ℓ cooperating but separated players. Each player i receives an input $x_i \in \mathcal{X}_i$ and produces an output $a_i \in \mathcal{A}_i$. They win if some predicate $V(a_1,\ldots,a_\ell,x_1,\ldots,x_\ell)$ is satisfied. To achieve this, they can agree on a joint strategy before the game starts, but then cannot communicate anymore.

Description of an ℓ-player non-local game G

- Input alphabet : $\underline{\mathcal{X}} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_\ell$. Output alphabet : $\underline{\mathcal{A}} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_\ell$.
- Game distribution $=$ P.d. on the queries : $\{T(\underline{x}) \in [0,1],\ \underline{x} \in \underline{\mathcal{X}}\}$.
- Game predicate $=$ Predicate on the answers and queries : $\{V(\underline{a},\underline{x}) \in \{0,1\},\ (\underline{a},\underline{x}) \in \underline{\mathcal{A}} \times \underline{\mathcal{X}}\}$.
- Players' strategy $=$ Conditional p.d. on the answers given the queries : $\{P(\underline{a}|\underline{x}) \in [0,1],\ (\underline{a},\underline{x}) \in \underline{\mathcal{A}} \times \underline{\mathcal{X}}\}$.

$\rightarrow$ Belongs to a set of "allowed strategies", depending on the kind of correlation resources that the players have (e.g. shared randomness, quantum entanglement, no-signalling boxes etc.)

Value of a game G over a set of allowed strategies $AS(\underline{\mathcal{A}}|\underline{\mathcal{X}})$

Maximum winning probability for players playing G with strategies $P \in AS(\underline{\mathcal{A}}|\underline{\mathcal{X}})$:

$$\omega_{AS}(G) = \max \left\{ \sum_{\underline{a}\in\underline{\mathcal{A}},\underline{x}\in\underline{\mathcal{X}}} T(\underline{x}) V(\underline{a},\underline{x}) P(\underline{a}|\underline{x}) \ : \ P \in AS(\underline{\mathcal{A}}|\underline{\mathcal{X}}) \right\}$$

$\rightarrow$ Bell functional of particular form : all coefficients in $[0,1]$

- **Classical correlations** : $P \in \mathrm{C}(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if

$$\forall\ \underline{x} \in \underline{\mathcal{X}},\ \forall\ \underline{a} \in \underline{\mathcal{A}},\ P(\underline{a}|\underline{x}) = \sum_{m \in \mathcal{M}} Q(m) P_1(a_1|x_1\, m) \cdots P_\ell(a_\ell|x_\ell\, m),$$

for some p.d. Q on $\mathcal{M}$ and some p.d.'s $P_i(\cdot|x_i\, m)$ on $\mathcal{A}_i$.

Some usual sets of allowed strategies

- **Classical correlations** : $P \in \mathrm{C}(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if

$$\forall\, \underline{x} \in \underline{\mathcal{X}},\ \forall\, \underline{a} \in \underline{\mathcal{A}},\ P(\underline{a}|\underline{x}) = \sum_{m\in\mathcal{M}} Q(m) P_1(a_1|x_1\, m) \cdots P_\ell(a_\ell|x_\ell\, m),$$

  for some p.d. Q on $\mathcal{M}$ and some p.d.'s $P_i(\cdot|x_i\, m)$ on $\mathcal{A}_i$.

- **Quantum correlations** : $P \in \mathrm{Q}(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if

$$\forall\, \underline{x} \in \underline{\mathcal{X}},\ \forall\, \underline{a} \in \underline{\mathcal{A}},\ P(\underline{a}|\underline{x}) = \langle \psi | M(x_1)_{a_1} \otimes \cdots \otimes M(x_\ell)_{a_\ell} | \psi \rangle,$$

  for some state $|\psi\rangle$ on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_\ell$ and some POVMs $M(x_i)$ on $\mathcal{H}_i$.

Some usual sets of allowed strategies

- **Classical correlations** : $P \in \mathrm{C}(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if
$$\forall\, \underline{x} \in \underline{\mathcal{X}},\ \forall\, \underline{a} \in \underline{\mathcal{A}},\ P(\underline{a}|\underline{x}) = \sum_{m\in\mathcal{M}} Q(m)P_1(a_1|x_1\, m)\cdots P_\ell(a_\ell|x_\ell\, m),$$
for some p.d. Q on $\mathcal{M}$ and some p.d.'s $P_i(\cdot|x_i\, m)$ on $\mathcal{A}_i$.

- **Quantum correlations** : $P \in \mathrm{Q}(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if
$$\forall\, \underline{x} \in \underline{\mathcal{X}},\ \forall\, \underline{a} \in \underline{\mathcal{A}},\ P(\underline{a}|\underline{x}) = \langle\psi|M(x_1)_{a_1}\otimes\cdots\otimes M(x_\ell)_{a_\ell}|\psi\rangle,$$
for some state $|\psi\rangle$ on $\mathcal{H}_1\otimes\cdots\otimes\mathcal{H}_\ell$ and some POVMs $M(x_i)$ on $\mathcal{H}_i$.

- **No-signalling correlations** : $P \in NS(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if
$$\forall\, I \subsetneq [\ell],\ \forall\, \underline{x} \in \underline{\mathcal{X}},\ \forall\, a_I \in \mathcal{A}_I,\ P(a_I|\underline{x}) = Q(a_I|x_I),$$
for some p.d.'s $Q(\cdot|x_I)$ on $\mathcal{A}_I$.

- **Sub-no-signalling correlations** : $P \in SNOS(\underline{\mathcal{A}}|\underline{\mathcal{X}})$ if
$$\forall\, I \subsetneq [\ell],\ \forall\, \underline{x} \in \underline{\mathcal{X}},\ \forall\, a_I \in \mathcal{A}_I,\ P(a_I|\underline{x}) \leqslant Q(a_I|x_I),$$
for some p.d.'s $Q(\cdot|x_I)$ on $\mathcal{A}_I$.

Remark : To check that a conditional p.d. is NS, it is enough to check that it satisfies the NS conditions on subsets of the form $I = [\ell]\setminus\{i\}$, i.e. that for each $1 \leqslant i \leqslant \ell$, the marginal of P on $\underline{\mathcal{A}}\setminus\mathcal{A}_i|\underline{\mathcal{X}}$ does not depend on $\mathcal{X}_i$. But this is probably false for SNOS.

Some remarks on no-signalling and sub-no-signalling correlations

Players sharing (sub-)no-signalling correlations : no limitation is assumed on their physical power, apart from the fact that they cannot signal information instantaneously from one another. In the no-signalling case, players are forced to always produce an output, whatever input they received, while in the sub-no-signalling case they are even allowed to abstain from doing so.

Some remarks on no-signalling and sub-no-signalling correlations

Players sharing (sub-)no-signalling correlations : no limitation is assumed on their physical power, apart from the fact that they cannot signal information instantaneously from one another. In the no-signalling case, players are forced to always produce an output, whatever input they received, while in the sub-no-signalling case they are even allowed to abstain from doing so.

Relating the NS and the SNOS values of games

- Clearly, for any game G, $\omega_{NS}(G) \leqslant \omega_{SNOS}(G)$. And there are examples of games G s.t. $\omega_{SNOS}(G) = 1$ while $\omega_{NS}(G) < 1$ (e.g. anti-correlation game).
- If G is a 2-player game, then $\omega_{NS}(G) = \omega_{SNOS}(G)$ (reason : for any 2-party *SNOS* correlation, there exists a 2-party *NS* correlation dominating it pointwise).
- If G is an ℓ-player game whose distribution T has full support, then $\omega_{NS}(G) < 1 \ \Rightarrow \ \omega_{SNOS}(G) < 1$ (more quantitatively : $\omega_{SNOS}(G) \geqslant 1 - \delta \ \Rightarrow \ \omega_{NS}(G) \geqslant 1 - \Gamma\delta$, where $\Gamma > 1$ only depends on T).

Parallel repetition of multi-player games

The ℓ players play n instances of G in parallel : Each player i receives its n inputs $x_i^{(1)},\ldots,x_i^{(n)}\in\mathcal{X}_i$ together and produces its n outputs $a_i^{(1)},\ldots,a_i^{(n)}\in\mathcal{A}_i$ together.
Product game distribution on $\underline{\mathcal{X}}^n$: $T^{\otimes n}\left(\underline{x}^n\right)=T\left(\underline{x}^{(1)}\right)\cdots T\left(\underline{x}^{(n)}\right)$.

Parallel repetition of multi-player games

The ℓ players play n instances of G in parallel : Each player i receives its n inputs $x_i^{(1)},\dots,x_i^{(n)} \in \mathcal{X}_i$ together and produces its n outputs $a_i^{(1)},\dots,a_i^{(n)} \in \mathcal{A}_i$ together.
Product game distribution on $\underline{\mathcal{X}}^n$: $T^{\otimes n}\left(\underline{x}^n\right) = T\left(\underline{x}^{(1)}\right)\cdots T\left(\underline{x}^{(n)}\right)$.

<u>Game $\mathbf{G^n}$</u> : The players win if they win all n instances of G.
$\rightarrow$ Product game predicate on $\underline{\mathcal{A}}^n \times \underline{\mathcal{X}}^n$: $V^{\otimes n}\left(\underline{a}^n,\underline{x}^n\right) = V\left(\underline{a}^{(1)},\underline{x}^{(1)}\right)\cdots V\left(\underline{a}^{(n)},\underline{x}^{(n)}\right)$.

Parallel repetition of multi-player games

The ℓ players play n instances of G in parallel : Each player i receives its n inputs $x_i^{(1)},\ldots,x_i^{(n)} \in \mathcal{X}_i$ together and produces its n outputs $a_i^{(1)},\ldots,a_i^{(n)} \in \mathcal{A}_i$ together.
Product game distribution on $\underline{\mathcal{X}}^n$: $T^{\otimes n}\left(\underline{x}^n\right) = T\left(\underline{x}^{(1)}\right)\cdots T\left(\underline{x}^{(n)}\right)$.

Game $\mathbf{G^n}$: The players win if they win all n instances of G.
$\rightarrow$ Product game predicate on $\underline{\mathcal{A}}^n \times \underline{\mathcal{X}}^n$: $V^{\otimes n}\left(\underline{a}^n,\underline{x}^n\right) = V\left(\underline{a}^{(1)},\underline{x}^{(1)}\right)\cdots V\left(\underline{a}^{(n)},\underline{x}^{(n)}\right)$.

Game $\mathbf{G^{t/n}}$: The players win if they win any t (or more) instances of G amongst the n.
$\rightarrow$ Game predicate on $\underline{\mathcal{A}}^n \times \underline{\mathcal{X}}^n$ defined as : $V^{t/n}\left(\underline{a}^n,\underline{x}^n\right) = 1$ if $\sum_{i=1}^n V\left(\underline{a}^{(i)},\underline{x}^{(i)}\right) \geqslant t$ and $V^{t/n}\left(\underline{a}^n,\underline{x}^n\right) = 0$ otherwise. In particular : $G^{n/n} = G^n$.

Parallel repetition of multi-player games

The ℓ players play n instances of G in parallel : Each player i receives its n inputs $x_i^{(1)},\ldots,x_i^{(n)}\in\mathcal{X}_i$ together and produces its n outputs $a_i^{(1)},\ldots,a_i^{(n)}\in\mathcal{A}_i$ together.
Product game distribution on $\underline{\mathcal{X}}^n$: $T^{\otimes n}(\underline{x}^n)=T(\underline{x}^{(1)})\cdots T(\underline{x}^{(n)})$.

Game $\mathbf{G^n}$: The players win if they win all n instances of G.
$\rightarrow$ Product game predicate on $\underline{\mathcal{A}}^n\times\underline{\mathcal{X}}^n$: $V^{\otimes n}(\underline{a}^n,\underline{x}^n)=V(\underline{a}^{(1)},\underline{x}^{(1)})\cdots V(\underline{a}^{(n)},\underline{x}^{(n)})$.

Game $\mathbf{G^{t/n}}$: The players win if they win any t (or more) instances of G amongst the n.
$\rightarrow$ Game predicate on $\underline{\mathcal{A}}^n\times\underline{\mathcal{X}}^n$ defined as : $V^{t/n}(\underline{a}^n,\underline{x}^n)=1$ if $\sum_{i=1}^n V(\underline{a}^{(i)},\underline{x}^{(i)})\geqslant t$ and $V^{t/n}(\underline{a}^n,\underline{x}^n)=0$ otherwise. In particular : $G^{n/n}=G^n$.

The value $\omega_{AS}(G^n)$, resp. $\omega_{AS}(G^{t/n})$, is the maximum winning probability for players playing G^n, resp. $G^{t/n}$, with strategies $P\in AS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$.

Parallel repetition of multi-player games

The ℓ players play n instances of G in parallel : Each player i receives its n inputs $x_i^{(1)},\ldots,x_i^{(n)} \in \mathcal{X}_i$ together and produces its n outputs $a_i^{(1)},\ldots,a_i^{(n)} \in \mathcal{A}_i$ together.
Product game distribution on $\underline{\mathcal{X}}^n$: $T^{\otimes n}(\underline{x}^n) = T(\underline{x}^{(1)})\cdots T(\underline{x}^{(n)})$.

Game $\mathbf{G^n}$: The players win if they win all n instances of G.
$\rightarrow$ Product game predicate on $\underline{\mathcal{A}}^n \times \underline{\mathcal{X}}^n$: $V^{\otimes n}(\underline{a}^n,\underline{x}^n) = V(\underline{a}^{(1)},\underline{x}^{(1)})\cdots V(\underline{a}^{(n)},\underline{x}^{(n)})$.

Game $\mathbf{G^{t/n}}$: The players win if they win any t (or more) instances of G amongst the n.
$\rightarrow$ Game predicate on $\underline{\mathcal{A}}^n \times \underline{\mathcal{X}}^n$ defined as : $V^{t/n}(\underline{a}^n,\underline{x}^n) = 1$ if $\sum_{i=1}^n V(\underline{a}^{(i)},\underline{x}^{(i)}) \geqslant t$ and $V^{t/n}(\underline{a}^n,\underline{x}^n) = 0$ otherwise. In particular : $G^{n/n} = G^n$.

The value $\omega_{AS}(G^n)$, resp. $\omega_{AS}(G^{t/n})$, is the maximum winning probability for players playing G^n, resp. $G^{t/n}$, with strategies $P \in AS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$.

Question : For AS being either C, Q, NS or $SNOS$, we clearly have

$$\omega_{AS}(G)^n \leqslant \omega_{AS}(G^n) \leqslant \omega_{AS}(G).$$

But in the case where $\omega_{AS}(G) < 1$, what is the true behavior of $\omega_{AS}(G^n)$? Does it decay to 0 exponentially (in n), and if so at which rate ? More generally, does $\omega_{AS}(G^{t/n})$ as well decay to 0 exponentially as soon as $t/n > \omega_{AS}(G)$?

Intuitively, why should de Finetti reductions be useful to understand the parallel repetition of multi-player games ?

Observation : Obviously, the game distribution $T_{\underline{X}}^{\otimes n}$ and the game predicate $V_{\underline{\mathcal{A}X}}^{\otimes n}$ of G^n are both permutation-invariant.

Intuitively, why should de Finetti reductions be useful to understand the parallel repetition of multi-player games ?

Observation : Obviously, the game distribution $T_{\underline{\mathcal{X}}}^{\otimes n}$ and the game predicate $V_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n}$ of G^n are both permutation-invariant.

Consequence : One can assume w.l.o.g. that the optimal winning strategy $P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n}$, in the set of allowed strategies $AS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$, for G^n is permutation-invariant as well. And hence,

$$T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \leqslant \mathrm{poly}(n) \int_{Q_{\underline{\mathcal{A}\mathcal{X}}}} F\left(T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n}, Q_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n} \right)^2 Q_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n} \, dQ_{\underline{\mathcal{A}\mathcal{X}}}.$$

Intuitively, why should de Finetti reductions be useful to understand the parallel repetition of multi-player games ?

Observation : Obviously, the game distribution $T_{\underline{\mathcal{X}}}^{\otimes n}$ and the game predicate $V_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n}$ of G^n are both permutation-invariant.

Consequence : One can assume w.l.o.g. that the optimal winning strategy $P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n}$, in the set of allowed strategies $AS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$, for G^n is permutation-invariant as well. And hence,

$$T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \leqslant \mathrm{poly}(n) \int_{Q_{\underline{\mathcal{A}\mathcal{X}}}} F\left(T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n}, Q_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n} \right)^2 Q_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n} \, dQ_{\underline{\mathcal{A}\mathcal{X}}}.$$

Goal : Show that the only p.d.'s $Q_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n}$ for which the fidelity weight is not exponentially small are those s.t. $Q_{\underline{\mathcal{A}\mathcal{X}}}$ is close to being of the form $T_{\underline{\mathcal{X}}} R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}}$ with $R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}} \in AS(\underline{\mathcal{A}}|\underline{\mathcal{X}})$. Because what happens when playing G^n with such strategy $R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}}^{\otimes n}$ is trivially understood.

Outline

Parallel repetition of (sub-)no-signalling multi-player games : some results

Parallel repetition of sub-no-signalling ℓ-player games

Let G be an ℓ-player game s.t. $\omega_{SNOS}(G) \leqslant 1-\delta$ for some $0<\delta<1$. Then, for any $n\in\mathbb{N}$ and $t \geqslant (1-\delta+\alpha)n$, $\omega_{SNOS}(G^n) \leqslant \left(1-\delta^2/5C_\ell^2\right)^n$ and $\omega_{SNOS}(G^{t/n}) \leqslant \exp\left(-n\alpha^2/5C_\ell^2\right)$, where $C_\ell = 2^{\ell+1}-3$.

Parallel repetition of (sub-)no-signalling multi-player games : some results

Parallel repetition of sub-no-signalling ℓ-player games

Let G be an ℓ-player game s.t. $\omega_{SNOS}(G) \leqslant 1-\delta$ for some $0<\delta<1$. Then, for any $n\in\mathbb{N}$ and $t \geqslant (1-\delta+\alpha)n$, $\omega_{SNOS}(G^n) \leqslant \left(1-\delta^2/5C_\ell^2\right)^n$ and $\omega_{SNOS}(G^{t/n}) \leqslant \exp\left(-n\alpha^2/5C_\ell^2\right)$, where $C_\ell = 2^{\ell+1}-3$.

Parallel repetition of no-signalling 2-player games

Let G be an 2-player game s.t. $\omega_{NS}(G) \leqslant 1-\delta$ for some $0<\delta<1$. Then, for any $n\in\mathbb{N}$ and $t \geqslant (1-\delta+\alpha)n$, $\omega_{NS}(G^n) \leqslant \left(1-\delta^2/27\right)^n$ and $\omega_{NS}(G^{t/n}) \leqslant \exp\left(-n\alpha^2/33\right)$.

Parallel repetition of (sub-)no-signalling multi-player games : some results

Parallel repetition of sub-no-signalling ℓ-player games

Let G be an ℓ-player game s.t. $\omega_{SNOS}(G) \leqslant 1-\delta$ for some $0<\delta<1$. Then, for any $n \in \mathbb{N}$ and $t \geqslant (1-\delta+\alpha)n$, $\omega_{SNOS}(G^n) \leqslant \left(1-\delta^2/5C_\ell^2\right)^n$ and $\omega_{SNOS}(G^{t/n}) \leqslant \exp\left(-n\alpha^2/5C_\ell^2\right)$, where $C_\ell = 2^{\ell+1}-3$.

Parallel repetition of no-signalling 2-player games

Let G be an 2-player game s.t. $\omega_{NS}(G) \leqslant 1-\delta$ for some $0<\delta<1$. Then, for any $n \in \mathbb{N}$ and $t \geqslant (1-\delta+\alpha)n$, $\omega_{NS}(G^n) \leqslant \left(1-\delta^2/27\right)^n$ and $\omega_{NS}(G^{t/n}) \leqslant \exp\left(-n\alpha^2/33\right)$.

Parallel repetition of no-signalling ℓ-player games with full support

Let G be an ℓ-player game whose input distribution T has full support, and s.t. $\omega_{NS}(G) \leqslant 1-\delta$ for some $0<\delta<1$. Then, for any $n \in \mathbb{N}$ and $t \geqslant (1-\delta+\alpha)n$, $\omega_{NS}(G^n) \leqslant \left(1-\delta^2/5C_\ell^2\Gamma^2\right)^n$ and $\omega_{NS}(G^{t/n}) \leqslant \exp\left(-n\alpha^2/5C_\ell^2\Gamma^2\right)$, where $C_\ell = 2^{\ell+1}-3$ and Γ is a constant which only depends on T.

Starting point : The optimal winning strategy $P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \in SNOS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$ for G^n satisfies

$$T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \leqslant \mathrm{poly}(n) \int_{Q_{\underline{\mathcal{A}\mathcal{X}}}} \widetilde{F}(Q_{\underline{\mathcal{A}\mathcal{X}}})^{2n} Q_{\underline{\mathcal{A}\mathcal{X}}}^{\otimes n} \, dQ_{\underline{\mathcal{A}\mathcal{X}}},$$

where $\widetilde{F}\left(Q_{\underline{\mathcal{A}\mathcal{X}}}\right) = \min\limits_{\emptyset \neq I \subsetneq [\ell]} \max\limits_{R_{\mathcal{A}_I|\mathcal{X}_I}} F\left(T_{\underline{\mathcal{X}}} R_{\mathcal{A}_I|\mathcal{X}_I}, Q_{\mathcal{A}_I \underline{\mathcal{X}}}\right)$.

$\rightarrow$ Follows from monotonicity of F under taking marginals + specific form of marginals of P + universal de Finetti reduction for conditional p.d.'s (Arnon-Friedman/Renner).

Starting point : The optimal winning strategy $P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \in SNOS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$ for G^n satisfies

$$T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \leqslant \mathrm{poly}(n) \int_{Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}} \widetilde{F}(Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}})^{2n} Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}^{\otimes n} \, dQ_{\underline{\mathcal{A}}\underline{\mathcal{X}}},$$

where $\widetilde{F}\left(Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}\right) = \min_{\emptyset \neq I \subsetneq [\ell]} \max_{R_{\mathcal{A}_I|\mathcal{X}_I}} F\left(T_{\underline{\mathcal{X}}} R_{\mathcal{A}_I|\mathcal{X}_I}, Q_{\mathcal{A}_I \underline{\mathcal{X}}}\right)$.

$\rightarrow$ Follows from monotonicity of F under taking marginals + specific form of marginals of P + universal de Finetti reduction for conditional p.d.'s (Arnon-Friedman/Renner).

Separating the "very-signalling" and the "not-too-signalling" parts in the integral :

Fix $0 < \varepsilon < 1$ and define $\mathcal{P}_\varepsilon = \left\{ Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \ : \ \max_{\emptyset \neq I \subsetneq [\ell]} \min_{R_{\mathcal{A}_I|\mathcal{X}_I}} \frac{1}{2} \| T_{\underline{\mathcal{X}}} R_{\mathcal{A}_I|\mathcal{X}_I} - Q_{\mathcal{A}_I \underline{\mathcal{X}}} \|_1 \leqslant \varepsilon \right\}$.

- $Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \notin \mathcal{P}_\varepsilon \ \Rightarrow \ \widetilde{F}\left(Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}\right)^2 \leqslant 1 - \varepsilon^2$.
- $Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \in \mathcal{P}_\varepsilon \ \Rightarrow \ \exists \ R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}} \in SNOS(\underline{\mathcal{A}}|\underline{\mathcal{X}}) : \ \frac{1}{2} \| T_{\underline{\mathcal{X}}} R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}} - Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \|_1 \leqslant C_\ell \varepsilon$.

$\rightarrow$ Technical lemma behind : If a conditional p.d. approximately satisfies each of the NS constraints, up to an error ε, then it is $C\varepsilon$-close to an exact SNOS p.d.

Parallel repetition of (sub-)no-signalling multi-player games : proof ingredients

Starting point : The optimal winning strategy $P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \in SNOS(\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n)$ for G^n satisfies

$$T_{\underline{\mathcal{X}}}^{\otimes n} P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n} \leqslant \mathrm{poly}(n) \int_{Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}} \widetilde{F}(Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}})^{2n} Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}^{\otimes n} \, dQ_{\underline{\mathcal{A}}\underline{\mathcal{X}}},$$

where $\widetilde{F}\left(Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}\right) = \min_{\emptyset \neq I \subsetneq [\ell]} \max_{R_{\mathcal{A}_I|\mathcal{X}_I}} F\left(T_{\underline{\mathcal{X}}} R_{\mathcal{A}_I|\mathcal{X}_I}, Q_{\mathcal{A}_I\underline{\mathcal{X}}}\right)$.

$\rightarrow$ Follows from monotonicity of F under taking marginals + specific form of marginals of P + universal de Finetti reduction for conditional p.d.'s (Arnon-Friedman/Renner).

Separating the "very-signalling" and the "not-too-signalling" parts in the integral :

Fix $0 < \varepsilon < 1$ and define $\mathcal{P}_\varepsilon = \left\{ Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \ : \ \max_{\emptyset \neq I \subsetneq [\ell]} \min_{R_{\mathcal{A}_I|\mathcal{X}_I}} \frac{1}{2} \| T_{\underline{\mathcal{X}}} R_{\mathcal{A}_I|\mathcal{X}_I} - Q_{\mathcal{A}_I\underline{\mathcal{X}}} \|_1 \leqslant \varepsilon \right\}$.

- $Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \notin \mathcal{P}_\varepsilon \ \Rightarrow \ \widetilde{F}\left(Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}}\right)^2 \leqslant 1 - \varepsilon^2$.
- $Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \in \mathcal{P}_\varepsilon \ \Rightarrow \ \exists \ R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}} \in SNOS(\underline{\mathcal{A}}|\underline{\mathcal{X}}) : \ \frac{1}{2} \| T_{\underline{\mathcal{X}}} R_{\underline{\mathcal{A}}|\underline{\mathcal{X}}} - Q_{\underline{\mathcal{A}}\underline{\mathcal{X}}} \|_1 \leqslant C_\ell \varepsilon$.

$\rightarrow$ Technical lemma behind : If a conditional p.d. approximately satisfies each of the NS constraints, up to an error ε, then it is $C\varepsilon$-close to an exact SNOS p.d.

Putting everything together : The winning probability when playing G^n with strategy $P_{\underline{\mathcal{A}}^n|\underline{\mathcal{X}}^n}$ is upper-bounded by $\mathrm{poly}(n)\left((1-\varepsilon^2)^n + (1-\delta+2C_\ell\varepsilon)^n\right)$.

It then just remains to choose $\varepsilon = C_\ell\left(\left(1+\delta/C_\ell^2\right)^{1/2} - 1\right)$ and get rid of the polynomial pre-factor in order to conclude.

Outline

Summary and open questions

Summary and open questions

- If ℓ players sharing sub-no-signalling correlations have a probability at most $1-\delta$ of winning a game G, then their probability of winning a fraction at least $1-\delta+\alpha$ of n instances of G played in parallel is at most $\exp(-nc_\ell\alpha^2)$, where $c_\ell > 0$ is a constant which depends only on ℓ.
  $\rightarrow$ Optimal dependence in α, even in the special case $\alpha = \delta$.

Summary and open questions

- If ℓ players sharing sub-no-signalling correlations have a probability at most $1-\delta$ of winning a game G, then their probability of winning a fraction at least $1-\delta+\alpha$ of n instances of G played in parallel is at most $\exp(-nc_\ell\alpha^2)$, where $c_\ell > 0$ is a constant which depends only on ℓ.
  $\rightarrow$ Optimal dependence in α, even in the special case $\alpha = \delta$.
- In the case $\ell = 2$, this is equivalent to the analogous concentration result for the no-signalling value of G (cf. Holenstein).

Summary and open questions

- If ℓ players sharing sub-no-signalling correlations have a probability at most $1-\delta$ of winning a game G, then their probability of winning a fraction at least $1-\delta+\alpha$ of n instances of G played in parallel is at most $\exp(-nc_\ell\alpha^2)$, where $c_\ell > 0$ is a constant which depends only on ℓ.
  $\rightarrow$ Optimal dependence in α, even in the special case $\alpha = \delta$.
- In the case $\ell = 2$, this is equivalent to the analogous concentration result for the no-signalling value of G (cf. Holenstein).
- In the case where the distribution of G has full support, this implies a similar concentration result for the no-signalling value of G, but with a highly game-dependent constant in the exponent (cf. Buhrman/Fehr/Schaffner and Arnon-Friedman/Renner/Vidick).
  $\rightarrow$ What about games where some of the potential queries are never asked to the players ?

Summary and open questions

- If ℓ players sharing sub-no-signalling correlations have a probability at most $1-\delta$ of winning a game G, then their probability of winning a fraction at least $1-\delta+\alpha$ of n instances of G played in parallel is at most $\exp(-nc_\ell\alpha^2)$, where $c_\ell > 0$ is a constant which depends only on ℓ.
  $\rightarrow$ Optimal dependence in α, even in the special case $\alpha = \delta$.
- In the case $\ell = 2$, this is equivalent to the analogous concentration result for the no-signalling value of G (cf. Holenstein).
- In the case where the distribution of G has full support, this implies a similar concentration result for the no-signalling value of G, but with a highly game-dependent constant in the exponent (cf. Buhrman/Fehr/Schaffner and Arnon-Friedman/Renner/Vidick).
  $\rightarrow$ What about games where some of the potential queries are never asked to the players ?
- **Classical case :** Exponential decay and concentration under parallel repetition for any 2-player game (Raz, Holenstein, Rao).
  Quantum case : Exponential decay under parallel repetition for any 2-player game with full support (Chailloux/Scarpa).
  $\rightarrow$ What about tackling the problem via de Finetti reductions ? Problem : classical and quantum conditions cannot be read off on the marginals...

Summary and open questions

- If ℓ players sharing sub-no-signalling correlations have a probability at most $1-\delta$ of winning a game G, then their probability of winning a fraction at least $1-\delta+\alpha$ of n instances of G played in parallel is at most $\exp(-nc_\ell\alpha^2)$, where $c_\ell > 0$ is a constant which depends only on ℓ.
  $\to$ Optimal dependence in α, even in the special case $\alpha = \delta$.
- In the case $\ell = 2$, this is equivalent to the analogous concentration result for the no-signalling value of G (cf. Holenstein).
- In the case where the distribution of G has full support, this implies a similar concentration result for the no-signalling value of G, but with a highly game-dependent constant in the exponent (cf. Buhrman/Fehr/Schaffner and Arnon-Friedman/Renner/Vidick).
  $\to$ What about games where some of the potential queries are never asked to the players ?
- **Classical case :** Exponential decay and concentration under parallel repetition for any 2-player game (Raz, Holenstein, Rao).
  Quantum case : Exponential decay under parallel repetition for any 2-player game with full support (Chailloux/Scarpa).
  $\to$ What about tackling the problem via de Finetti reductions ? Problem : classical and quantum conditions cannot be read off on the marginals...
- Using flexible de Finetti reductions to prove the (weakly) multiplicative or additive behavior of certain quantities appearing in QIT : work in progress...

References

- **P. Diaconis, D. Freedman**, "Finite exchangeable sequences".
- **M. Christandl, R. König, G. Mitchison, R. Renner**, "One-and-a-halh quantum de Finetti theorems", arXiv :quant-ph/0602130.
- **M. Christandl, R. König, R. Renner**, "Post-selection technique for quantum channels with applications to quantum cryptography", arXiv[quant-ph] :0809.3019.
- **R. Arnon-Friedman, R. Renner**, "de Finetti reductions for correlations", arXiv[quant-ph] :1308.0312.
- **T. Holenstein**, "Parallel repetition : simplifications and the no-signaling case", arXiv :cs/0607139.
- **H. Buhrman, S. Fehr, C. Schaffner**, "On the Parallel Repetition of Multi-Player Games : The No-Signaling Case", arXiv[quant-ph] :1312.7455.
- **R. Arnon-Friedman, R. Renner, T. Vidick**, "Non-signalling parallel repetition using de Finetti reductions", arXiv[quant-ph] :1411.1582.
- **C. Lancien, A. Winter**, "Parallel repetition and concentration for (sub-)no-signalling games via a flexible constrained de Finetti reduction", arXiv[quant-ph] :1506.07002.
- **R. Raz**, "A parallel repetition theorem".
- **A. Rao**, "Parallel repetition in projection games and a concentration bound".
- **A. Chailloux, G. Scarpa**, "Parallel repetition of free entangled games : simplification and improvements", arXiv[quant-ph] :1410.4397.